中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder：

申　　請　　日 ： 西元 2003 年 04 月 03 日
Application Date

申　請　案　號 ： 092107680
Application No.

申　　請　　人 ： 上元科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2003 年 7 月 24 日
Issue Date

發文字號： 09220747140
Serial No.

發明專利說明書

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：_____ ※IPC 分類：_____

※ 申請日期：_____

壹、發明名稱

(中文) 無線區域網路之加／解密裝置及其方法

(英文)

貳、發明人（共 3 人）

發明人 1 （如發明人超過一人，請填**說明書發明人續頁**）

姓名：(中文) 鄭聖源

(英文) SHENG-YUAN CHENG

住居所地址：(中文) 新竹縣竹北市民權街 55 號 2 樓

(英文)

國籍：(中文) 中華民國 (英文) REPUBLIC OF CHINA

參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填**說明書申請人續頁**）

姓名或名稱：(中文) 上元科技股份有限公司

(英文) ADMTEK INCORPORATED

住居所或營業所地址：(中文) 新竹縣科學工業園區工業東九路 9 號 1 樓

(英文) 1F, NO. 9, INDUSTRY E. 9TH RD., SCIENCE-BASED INDUSTRIAL PARK, HSINCHU, TAIWAN, R.O.C.

國　籍：(中文) 中華民國 (英文) REPUBLIC OF CHINA

代表人：(中文) 盧崑瑞 (英文)

發明人 2

姓名：(中文) 劉榮煜

(英文) YUNG-YU LIU

住居所地址：(中文) 新竹縣芎林鄉上山村上山 146 號

(英文)

國籍：(中文) 中華民國 (英文) REPUBLIC OF CHINA

發明人 3

姓名：(中文) 方信雄

(英文) HSIN-HSIUNG FANG

住居所地址：(中文) 台南縣安定鄉海寮村 205 號之 8

(英文)

國籍：(中文) 中華民國 (英文) REPUBLIC OF CHINA

肆、中文發明摘要

本發明揭示一種無線區域網路之加／解密裝置及方法。本發明之加／解密裝置係電氣連接至一主系統。該加／解密裝置包含一資料接收單元、一資料傳送單元、一解密判斷單元、一加密判斷單元、一硬體加／解密單元、一第一判斷單元及一第二判斷單元。該硬體加／解密單元包含一第一加／解密對應表，而該主系統則包含一第二加／解密對應表。該第一及該第二加／解密對應表之內容包含其可加／解密之工作站代碼、加／解密演算法代碼及鑰匙。當該硬體加／解密單元可加／解密一訊框時，由該硬體加／解密單元進行加／解密，否則由該主系統進行加／解密。

伍、英文發明摘要

陸、(一)、本案指定代表圖為：第 4 圖

(二)、本代表圖之元件代表符號簡單說明：

20	加／解密裝置	22	硬體加／解密單元
24	主系統	26	資料接收單元
28	解密判斷單元	29	第一判斷單元
30	應用程式	32	加密判斷單元
33	第二判斷單元	34	資料傳送單元

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

捌、聲明事項

☐ **本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：** _____

☑ **本案已向下列國家（地區）申請專利，申請日期及案號資料如下：**

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1. 本案在向中華民國提出申請前未曾向其他國家提出申請專利。
2. _____
3. _____

☐ **主張專利法第二十四條第一項優先權：**

【格式請依：受理國家（地區）；日期；案號　順序註記】

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

☐ **主張專利法第二十五條之一第一項優先權：**

【格式請依：申請日；申請案號　順序註記】

1. _____
2. _____
3. _____

☐ **主張專利法第二十六條微生物：**

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1. _____
2. _____
3. _____

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1. _____
2. _____
3. _____

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

【發明所屬之技術領域】

本發明係關於一種無線區域網路之加／解密裝置及方法，特別是關於一種由硬體電路加／解密資料之加／解密裝置及方法。

【先前技術】

由於可攜式電子裝置（例如：手機、個人數位助理器及筆記型電腦等）普及率的快速成長，無線區域網路對今日的電腦及通訊工業來講，已成為一項重要的觀念及技術。在無線區域網路的架構中，電腦主機不需要像在傳統的有線區域網路裡必需保持固定在網路架構中的某個節點上，而可以在任意的時間作空間上的移動，也能對網路上的資料作任意的擷取。

在無線通訊中，傳輸資料被竊聽是常見的現象。由於無線電波的廣播特性，任何欲竊聽者只要將其竊聽器的接收頻率調至傳送頻率即可順利進行竊聽的工作。為了解決這個問題，IEEE 802.11標準中制定了一個與有線區域網路具同等功效的資料保密演算法，可保護無線區域網路之授權使用者免於被竊聽的煩惱。有線區域網路上要進行竊聽的工作至少要連接到線上，這種不方便性在某種程度上也可說是一種安全屬性。無線區域網路雖然不具備這種特有的安全屬性，然IEEE 802.11採用了有線等效保密演算法（wired equivalent privacy algorithm，WEP），以便提供與此功能相當的安全性。

WEP 運作原理係將原始二進位資料經過加密演算處理後，將其資訊內容隱藏起來，該原始二進位資料稱為原文（plaintext，簡稱P），而經過加密處理的資料則稱為密文（ciphertext，簡稱C）。密碼演算法（cryptographic algorithm，或稱為cipher)就是一種用來對資料進行加密及解密的數學函式。近代密碼演算法大都採用鑰匙（key，簡稱 k）技術來進行加密及解密的工作。加密演算法（Encryption function，簡稱 E）處理原文 P 後得到密文C：

Ek（P）=C

欲還原時，解密演算法（Decryption function，簡稱 D）利用相同的鑰匙處理密文C後得到原文P：

Dk（C）=Dk（Ek（P））= P

圖1係先前技術使用於無線區域網路之電子裝置之功能方塊圖。如圖1所示，電子裝置10包含一資料接收單元12、一解密判斷單元14、一硬體加／解密單元16及一加密判斷單元19。該電子裝置10係連接至一應用程式18，以便資料傳輸之進行。硬體加／解密單元16包含一加／解密對應表，記錄其可以加／解密之起始工作站（source station，簡稱SA）位址、加／解密演算法及鑰匙，而起始工作站位址（SA）是指產生一由資料接收單元12接收之訊框之工作站位址。

圖2係先前技術之無線區域網路之解密流程圖。當資料接收單元12收到來自一起始工作站（圖未顯示）之訊框時，即將該訊框送至解密判斷單元14。該解密判斷單元14

根據該訊框之表頭判斷是否需要進行解密(即判斷該訊框係經加密之密文或係未經加密之原文)。如該訊框係未經加密之原文，則該訊框將被送至應用程式18，否則該訊框將被送至硬體加／解密單元16。當該訊框被傳送至硬體加／解密單元16時，如該訊框中記載之起始工作站位址存在硬體加／解密單元16之加／解密對應表內，則硬體加／解密單元16即利用對應該起始工作站之解密演算法及鑰匙將該訊框解密為原文後傳送至應用程式18。然而，當該訊框中記載之起始工作站位址並未儲存在硬體加／解密單元16之加／解密對應表內，則硬體加／解密單元16便無法處理該訊框。

圖3係先前技術之無線區域網路之加密流程圖。當應用程式18欲傳送一資料至一目的工作站時，即在該資料加上用以分辨是否加密之表頭與目的地工作站位址。在該資料被包裝為一訊框後，該訊框被傳送至加密判斷單元19。該加密判斷單元19根據該訊框之表頭判斷其是否需要進行加密。如該訊框是需原文傳送，則該訊框將被送至資料傳送單元17，否則該訊框將被傳送至硬體加／解密單元16。

當該訊框被傳送至硬體加／解密單元16時，如該訊框中記載之目的工作站位址存在硬體加／解密單元16之加／解密對應表內，則硬體加／解密單元16即利用對應該目的工作站之加密演算法及鑰匙對該訊框進行加密後傳送至資料傳送單元17。然而，當該訊框中記載之目的工作站位址並未儲存在硬體加／解密單元16之加／解密對應表

內，則硬體加／解密單元16便無法處理該訊框。

近年來，新的加／解密演算法陸續地推出以確保無線區域網路資料傳輸之安全性，而由於硬體解密單元16係採硬體電路設計，因此無法對儲存於硬體加／解密單元16之解密演算法及鑰匙進行更新，因而限制電子裝置10之應用範圍。而為了適用新推出之演算法，採用硬體加／解密單元16之電子裝置10必須隨時更新其採用之解密單元，如此將增加電子裝置10之使用成本。再者，硬體解密單元16之電路必須重新設計方可納入新推出之演算法，如此亦大大地將增加硬體解密單元16之製作成本。

【發明內容】

本發明之第一目的係為解決先前技術無法進行更新以納入新推出之加／解密演算法之問題而提供一種在無線區域網路之加／解密裝置，其係利用一硬體加／解密單元以提升加／解密運算之速度，且利用一主系統之運算能力以納入新推出的加／解密演算法。

本發明之第二目的提供一種在無線區域網路之加／解密裝置，其係利用一硬體加／解密單元以提升加／解密運算之速度，且利用一可程式化加／解密單元之運算能力以納入新推出的加／解密演算法。

本發明之第三目的係為提供一種在無線區域網路之加密方法，其可增加資料之加密彈性及降低硬體加密單元之設計複雜度。

本發明之第四目的係為提供一種在無線區域網路之解

密方法，其可增加資料之解密彈性及降低硬體加解密單元之設計複雜度。

為達成上述目的並解決先前技術之缺點，本發明揭示一種無線區域網路之加／解密裝置，電氣連接至一主系統。該主系統包含一第二加／解密對應表，該第二加／解密對應表之記錄內容包含其可以加／解密之工作站代碼、加／解密演算法代碼及鑰匙。該加／解密裝置包含一用以接收訊框之資料接收單元、一電氣連接於該資料接收單元之解密判斷單元、一硬體加／解密單元、一電氣連接於該解密判斷單元和該硬體加／解密單元之第一判斷單元、一電氣連接於該主系統之加密判斷單元，一電氣連接於該硬體加／解密單元和該加密判斷單元之第二判斷單元、以及一用以傳送訊框之資料傳送單元。該硬體加／解密單元係依至少一個加／解密演算法所製作之電路，其包含一第一加／解密對應表。該第一加／解密對應表之記錄內容包含其可以加／解密之工作站代碼、加／解密演算法代碼及鑰匙。該第一判斷單元係用於判斷由該資料接收單元接收之加密訊框應由該硬體加／解密單元或該主系統進行解密。該第二判斷單元係用於判斷該應加密訊框應由該硬體加／解密單元加密或該應加密訊框已由主系統加密直接傳送至該資料傳送單元。

本發明之加／解密裝置之另一實施例包含一硬體加／解密單元、一可程式化加／解密單元、一用於傳送訊框之資料傳送單元、一用於接收訊框之資料接收單元、一電氣

連接於該資料接收單元之解密判斷單元、一電氣連接於該解密判斷單元和硬體加／解密單元之第一判斷單元，用於判斷由該資料接收單元接收之加密訊框應由該硬體加／解密單元或該可程式化加／解密單元進行解密、一電氣連接於該可程式化加／解密單元之加密判斷單元、以及一電氣連接於該加密判斷單元和該硬體加／解密單元之第二判斷單元，用於判斷該應加密訊框應由該硬體加／解密單元加密或該應加密訊框已由可程式化加／解密單元加密直接傳送至該資料傳送單元。

本發明之無線區域網路之解密方法首先判斷收到之訊框為密文或原文。若該訊框為密文，則判斷一由解密演算法所製作之硬體解密單元是否可解密。該硬體解密單元可解密該訊框，則由該硬體解密單元進行解密，否則將該訊框傳送至一可程式化解密單元進行解密。

本發明之無線區域網路之加密方法首先判斷要傳送之訊框是否需要加密。若需加密，判斷一由加密演算法所製作之硬體加密單元可否加密。若該硬體加密單元可加密該訊框，則由該硬體加密單元進行加密後傳送該訊框至一目的工作站，否則由一可程式加密單元進行加密後傳送該訊框至該目的工作站。

由於本發明可隨時以程式更新第二加／解密對應表及對應之加／解密演算法及鑰匙，以納入最新推出之／解密算法，因此相較於先前技術，本發明具有下列之優點：

(1) 本發明之加／解密裝置之應用範圍不會受到限制，

且可隨著加／解密技術的進步而不斷延展。

(2) 由於在不需更新整個硬體加／解密單元即可納入新的加／解密演算法，因此可降低成本。

(3) 由於本發明之硬體加／解密單元和主系統係緊密地配合著，設計者可彈性分配硬體和程式空之工作比重，因此本發明之設計具有較高之彈性。

(4) 本發明之裝置可利用主系統之資源擴充可加/解密的對象，而不受硬體加/解密對應表的限制。

【實施方式】

本發明將在此參考圖式更加詳細地說明，其中較佳實施例將出現在下列之敘述中。然而，本發明可以許多不同形式具體化，且應不限於較佳實施例所揭示者。更確切地說，這些較佳實施例的提供僅係用以使本發明之揭示更加完整及徹底，且將完全地表達本發明之範圍給熟悉該項技藝者。請瞭解當敘述一元件（例如一解密判斷單元）"電氣連接於另一元件"時，其可為直接電氣連接於該另一元件，也可以具有介於中間之元件存在。相對地，當敘述一元件係"直接電氣連接於"另一元件時，則沒有任何介於中間的元件存在。此外，說明書中敘述之工作站（Station）係指任何擁有 IEEE 802.11的MAC層和PHY層介面之設備。工作站代碼係為一工作站之辨識碼，例如工作站之位址。演算法代碼係為一演算法之辨識碼。目地的工作站是一訊框（frame）之最終目的地工作站，而起始工作站是產生一訊框之工作站。

圖4係本發明之加／解密裝置20之功能方塊圖。該加／解密裝置20係電氣連接於一主系統（host）24（例如一工作站或一個人電腦）。如圖4所示，本發明之加／解密裝置20包含一用以接收訊框之資料接收單元26、一電氣連接於該資料接收單元26之解密判斷單元28、一硬體加／解密單元22、一電氣連接於該解密判斷單元28和該硬體加／解密單元22之第一判斷單元29、一電氣連接於該主系統24之加密判斷單元32，一電氣連接於該硬體加／解密單元22和該加密判斷單元33之第二判斷單元33、以及一用以傳送訊框之資料傳送單元34。第一判斷單元29係用於判斷由該資料接收單元26接收之加密訊框應由該硬體加／解密單元22或該主系統24進行解密，而第二判斷單元33係用於判斷一應加密訊框應由該硬體加／解密單元22加密或已由該主系統加密。

該硬體加／解密單元22係依至少一個加／解密演算法所製作之電路，包含一內建之第一加／解密對應表，如表1所示。該第一加／解密對應表之記錄內容包含其可進行加／解密之工作站代碼、加／解密演算法代碼及鑰匙。如果該硬體加／解密單元22係依單一加／解密演算法所製作之電路，則該第一加／解密對應表可只包含工作站代碼及鑰匙二個欄位。

該主系統24包含一第二加／解密對應表，其格式大略相同於第一加／解密對應表。和第一加／解密對應表最大的差別在於主系統24之第二加／解密對應表因係儲存於

主系統24之記憶體內，因此其容量較大，可隨工作站數量之增加而以程式（可為軟體或韌體）不斷更新或增加。此外，第二加／解密對應表在設計上可選擇包含第一加／解密對應表之全部內容。

表1

工作站代碼	加／解密演算法代碼	鑰匙
SA0	E／D0	K0
SA1	E／D1	K1
SA2	E／D2	K2
SA3	E／D3	K3
SA4	E／D4	K4
…	…	…

當資料接收單元26收到來自一起始工作站（圖未顯示）之訊框（frame）時，即將該訊框傳送至解密判斷單元28。該解密判斷單元28根據該訊框之表頭判斷是否需要進行解密（即判斷該訊框係經加密之密文或係未經加密之原文）。如該訊框係經加密之密文（即一加密訊框），則該訊框將被送至第一判斷單元29，否則即傳送該訊框至該主系統24，由應用程式30處理該原文。

第一判斷單元29可根據該訊框之內容（例如發送該訊框之起始工作站代碼）判斷該硬體加／解密單元22可否對該訊框解密。例如，比對該加密訊框中記載之起始工作站代碼是否儲存在該第一加／解密對應表內。如答案是肯定的，則表示該硬體加／解密單元22可將加密該訊框解密成

原文，該第一判斷單元29即將該加密訊框傳送至硬體加／解密單元22。該硬體加／解密單元22即利用第一加／解密對應表中對應該起始工作站代碼之解密演算法及鑰匙將該加密訊框解密成為原文。

當該加密訊框中記載之起始工作站代碼並未儲存於硬體加／解密單元22之第一加／解密對應表內，則表示該硬體加／解密單元22無法對該加密訊框進行解密，此時該第一判斷單元29即將該加密訊框傳送至該主系統24進行第二階段之解密。該主系統24利用第二加／解密對應表中對應該起始工作站代碼之解密演算法及鑰匙將該加密訊框解密為原文，再傳送至應用程式30。

類似解密的原理，當該應用程式30欲傳送一資料至一目的工作站時，該主系統24即在該資料加上用以分辨是否加密之表頭與目的地工作站代碼。在該資料被包裝為一訊框後，該訊框被傳送至加密判斷單元32。該加密判斷單元32根據該訊框之表頭判斷其是否需要進行加密。如該訊框是需原文傳送，則該訊框將被傳送至該加密判斷單元32。該加密判斷單元32收到該訊框後，即判斷該訊框是否需要加密，若需加密即將該訊框傳送至該第二判斷單元33，若不需加密即將該訊框傳送至資料傳送單元34。

對一應加密訊框之傳送而言，由於主系統24之第二加／解密對應表包含了硬體加／解密單元22之第一加／解密對應表及對應每一工作站代碼之加／解密演算法及鑰匙，因此主系統24可據以比對該應加密訊框欲傳送之目的

工作站代碼。如果該目的工作站代碼並未儲存於硬體加／解密單元22之第一加／解密對應表內，該主系統24即利用第二加／解密對應表內對應該目的地工作站代碼之加密演算法及鑰匙進行加密以得到密文，並經由加密判斷單元32將應加密訊框傳送至資料傳送單元34。

如果該目的工作站代碼係儲存於硬體加／解密單元22之第一加／解密對應表，即表示硬體加／解密單元22可以對該應加密訊框進行加密。此時，主系統24並不進行該應加密訊框之加密，而將該應加密訊框傳送至該加密判斷單元32。該加密判斷單元32收到該應加密訊框後，即將該應加密訊框傳送至該第二判斷單元33。該第二判斷單元33判斷該應加密訊框是否需要由該硬體加／解密單元22進行加密（即判斷該訊框是否已由該主系統24進行加密），若該應加訊框尚未由該主系統24加密，該第二判斷單33即將該應加密訊框傳送至該硬體加／解密單元22。若該應加密訊框已由該主系統24加密，即將該應加密訊框傳送至該資料傳送單元34。該硬體加／解密單元22收到該應加密訊框時，即利用其第一加／解密對應表內對應該目的工作站代碼之加密演算法及鑰匙對該應加訊框進行加密以得到密文，並傳送至該資料傳送單元34。

圖5係本發明之加／解密裝置之另一實施例之功能方塊圖。如圖5所示，本發明之加／解密裝置40包含一硬體加／解密單元42、一可程式化加／解密單元44、一用於傳送訊框之資料傳送單元54、一用於接收訊框之資料接收單

元46、一電氣連接於該資料接收單元46之解密判斷單元48、一電氣連接於該解密判斷單元48和硬體加／解密單元42之第一判斷單元49，一電氣連接於該可程式化加／解密單元44之加密判斷單元52、以及一電氣連接於該加密判斷單元52和該硬體加／解密單元42之第二判斷單元53。第一判斷單元49係用於判斷由該資料接收單元46接收之訊框應由該硬體加／解密單元42或該可程式化加／解密單元44進行解密，而第二判斷單元53係用於判斷該訊框應由該硬體加／解密單元42加密或傳送至該資料傳送單元54。

該硬體加／解密單元42係依至少一個加／解密演算法所製作之電路。該硬體加／解密單元42包含一第一加／解密對應表，該第一加／解密對應表之記錄內容包含其可以加／解密之工作站代碼、加／解密演算法及鑰匙。如果該硬體加／解密單元42係依單一加／解密演算法所製作之電路，則該第一加／解密對應表可只包含工作站代碼及鑰匙二個欄位。

該可程式化加／解密單元44係由一可程式邏輯元件或一嵌入式系統（Embedded system）構成。該可程式化加／解密單元44包含一第二加／解密對應表，該第二加／解密對應表之記錄內容包含其可以加／解密之工作站代碼、加／解密演算法及鑰匙。第二加／解密對應表及其記錄之加／解密演算法及鑰匙係可由程式予以更新或增加，且設計上可包含第一加／解密對應表。

當資料接收單元46收到來自一起始工作站（圖未顯示）

之訊框時，即將該訊框傳送至解密判斷單元48。該解密判斷單元48根據該訊框之表頭判斷是否需要進行解密。如該訊框係經加密之密文，則該訊框將被送至第一判斷單元49，否則即經由該可程式化加／解密單元44傳送至該應用程式50，由應用程式50處理該原文。

若該訊框為一加密訊框，該第一判斷單元49根據該加密訊框之內容（例如發送該訊框之起始工作站代碼）判斷該硬體加／解密單元42可否對該加密訊框解密，即比對該加密訊框中記載之起始工作站代碼是否儲存在該第一加／解密對應表內。如答案是肯定的，則表示該硬體加／解密單元42可將該加密訊框解密為原文，該第一判斷單元49即將該加密訊框傳送至該硬體加／解密單元42。該硬體加／解密單元42即利用第一加／解密對應表中對應該起始工作站代碼之解密演算法及鑰匙將該加密訊框解密成為原文後傳送至該應用程式50。

當該加密訊框中記載之起始工作站代碼並未儲存於硬體加／解密單元42之第一加／解密對應表內，則表示該硬體加／解密單元42無法對該加密訊框進行解密，此時該第一判斷單元49即將該加密訊框傳送至該可程式化加／解密單元44進行第二階段之解密。該可程式化加／解密單元44利用第二加／解密對應表中對應該起始工作站代碼之解密演算法及鑰匙將該加密訊框解密為原文，再傳送至應用程式50。

類似解密的原理，當該應用程式50欲傳送一資料至一

目的工作站時，可程式化加／解密單元44即在該資料加上用以分辨是否加密之表頭與目的地工作站代碼後傳送至加密判斷單元32。該加密判斷單元52根據該訊框之表頭判斷其是否需要進行加密，如該訊框是需原文傳送，則該訊框將被傳送至資料傳送單元54。否則將該訊框傳送至第二判斷單元53。

當該訊框需以密文傳送時（即為一應加密訊框），由於可程式化加／解密單元44之第二加／解密對應表包含了硬體加／解密單元42之第一加／解密對應表及對應每一工作站代碼之加／解密演算法及鑰匙，因此可程式化加／解密單元44可據以比對該應加密訊框欲傳送之目的工作站代碼。如果該目的工作站代碼並未儲存於硬體加／解密單元42之第一加／解密對應表內，該可程式化加／解密單元44即利用第二加／解密對應表內對應該目的地工作站代碼之加／解密演算法及鑰匙進行該應加密訊框之加密以得到密文，並經由加密判斷單元52將應加密訊框傳送至資料傳送單元54。

如果該目的工作站代碼係儲存於硬體加／解密單元42之第一加／解密對應表，即表示硬體加／解密單元42可以對該應加密訊框進行加密。此時，可程式化加／解密單元44並不進行該應加密訊框之加密，而將該應加密訊框傳送至該加密判斷單元52。該加密判斷單元52收到該應加密訊框後，即將該應加密訊框傳送至該第二判斷單元53。該第二判斷單元53判斷該應加密訊框是否需要由該硬體加／

解密單元42進行加密(即判斷該訊框是否已由可程式化加／解密單元44進行加密)。若該應加密訊框尚未由可程式化加／解密單元44加密，該第二判斷單53即將該應加密訊框傳送至該硬體加／解密單元42。若該應加密訊框已由可程式化加／解密單元44加密，即將該應加密訊框傳送至該資料傳送單元54。該硬體加／解密單元42收到該應加密訊框時，即利用第一加／解密對應表內應該目的工作站代碼之加密演算法及鑰匙對該應加密訊框進行加密以得到密文，並傳送至該資料傳送單元54。

圖6係本發明之解密方法之流程圖。如圖6所示，在收到一訊框後，本發明之解密方法首先判斷該訊框為加密之密文或未加密之原文。若該訊框為加密之密文，則判斷一硬體解密單元可否進行該訊框之解密。若答案是肯定的，則傳送該訊框至該硬體解密單元，由該硬體解密單元進行該訊框之解密，否則由一可程式化解密單元透過其內部程式將該訊框解密為原文。

該硬體解密單元係依至少一個加密演算法所製作之電路包含一第一解密對應表，該可程式化加密單元則包含一第二解密對應表，且該第一和第二解密對應表之記錄內容包含其可以解密之工作站代碼及鑰匙。在本發明之解密方法中，判斷該硬體解密單元可否解密該訊框係比對發出該訊框之起始工作站代碼是否儲存於該硬體解密單元內部之第一解密對應表內。若該起始工作站代碼存在於該第一解密對應表內，即表示該硬體解密單元可以將該訊框解密

為原文。當該訊框傳送至該硬體解密單元時，即依第一解密對應表內對應該起始工作站代碼之解密演算法及鑰匙對該訊框進行解密。

該可程式化解密單元可由一工作站、一個人電腦、一可程式邏輯元件或一嵌入式系統構成。設計上該第二解密對應表包含該第一解密對應表及其記錄之解密演算法及鑰匙。此外該第二解密對應表可由程式予以更新或增加。當該可程式化解密單元收到該訊框時，即依第二解密對應表內對應該起始工作站代碼之解密演算法及鑰匙對該訊框進行解密。

圖7係本發明之加密方法之流程圖。當要傳送資料至一目的工作站時，本發明之加密方法首先由一可程式化加密單元將該資料包裝為一訊框，且判斷該資料是否要加密。若答案是否定的，則傳送該訊框至該目的工作站。若答案是肯定的，則先判斷一硬體加密單元可否加密該訊框。若答案是肯定的，則傳送該訊框至該硬體加密單元，該訊框即由該硬體加密單元加密後傳送至該目的工作站，否則即由該可程式化加密單元透過其內部程式將該訊框加密後傳送至該目的工作站。

該硬體加密單元係依至少一個加密演算法所製作之電路，其包含一第一加密對應表，該可程式化加密單元則包含一第二加密對應表，該第一和第二加密對應表之記錄內容包含其可以加密之工作站代碼及鑰匙。在本發明之加密方法中，判斷該硬體加密單元可否加密該訊框係比對該目

的工作站代碼是否儲存於該硬體加密單元內部之第一加密對應表內。若該目的工作站代碼存在於該第一加密對應表內，即表示該硬體加密單元可以將該訊框加密成密文。當該訊框傳送至該硬體加密單元時，即依第一加密對應表內對應該目的工作站代碼之加密演算法及鑰匙對該訊框進行加密。

該可程式化加密單元可由一工作站、一個人電腦、一可程式邏輯元件或一嵌入式系統構成。設計上該第二加密對應表可包含該第一加密對應表。此外該第二加密對應表可由程式予以更新。當該硬體加密單元無法加密該訊框時，該可程式化加密單元即自行依第二加密對應表內對應該目的工作站代碼之加密演算法及鑰匙對該訊框進行加密。

由於本發明可隨時以程式更新第二加／解密對應表，以納入最新推出之加／解密算法，因此相較於先前技術，本發明具有下列之優點：

(1) 本發明之加／解密裝置之應用範圍不會受到限制，且可隨著加／解密技術的進步而不斷延展。

(2) 由於在不需更新整個硬體加／解密單元即可納入新的加／解密演算法，因此可降低成本。

(3) 由於本發明之硬體加／解密單元和主系統（或可程式化加／解密單元）係緊密地配合著，設計者可彈性分配硬體和程式空之工作比重，因此本發明之設計具有較高之彈性。

(4)本發明之裝置可利用主系統之資源擴充可加/解密的對象，而不受硬體加/解密對應表的限制。

【圖式之簡單說明】

本發明將依照後附圖式來說明，其中：

圖1係先前技術之解密裝置之功能方塊圖；

圖2係先前技術之解密裝置之流程圖；

圖3係先前技術之解密裝置之流程圖；

圖4本發明之加／解密裝置之功能方塊圖；

圖5係本發明之加／解密裝置之另一實施例之功能方塊圖；

圖6係本發明之解密方法之流程圖；及

圖7係本發明之加密方法之流程圖。

元件符號說明

10	電子裝置	12	資料接收單元
14	解密判斷單元	16	硬體解密單元
18	應用程式	19	加密判斷單元
20	加／解密裝置	22	硬體加／解密單元
24	主系統	26	資料接收單元
28	解密判斷單元	29	第一判斷單元
30	應用程式	32	加密判斷單元
33	第二判斷單元	34	資料傳送單元
40	加／解密裝置	42	硬體加／解密單元
44	可程式化加／解密單元	46	資料接收單元
48	解密判斷單元	49	第一判斷單元

50 應用程式　　52 加密判斷單元

53 第二判斷單元　　54 資料傳送單元

本發明之技術內容及技術特點已揭示如上，然而熟悉本項技術之人士仍可能基於本發明之教示及揭示而作種種不背離本發明精神之替換及修飾。因此，本發明之保護範圍應不限於實施例所揭示者，而應包括各種不背離本發明之替換及修飾，並為本發明之申請專利範圍所涵蓋。

拾、申請專利範圍

1. 一種無線區域網路之加／解密裝置，電氣連接至一主系統，該主系統包含一第二加／解密對應表，該第二加／解密對應表之記錄內容包含該主系統可以加／解密之工作站代碼、加／解密演算法代碼及鑰匙，該加／解密裝置包含：

一資料接收單元，用於接收訊框；

一資料傳送單元，用於傳送訊框；

一硬體加／解密單元，其係依至少一個加／解密演算法所製作之電路，該硬體加／解密單元包含一第一加／解密對應表，該第一加／解密對應表之記錄內容包含該硬體加／解密單元可以加／解密之工作站代碼、加／解密演算法代碼及鑰匙；

一第一判斷單元，電氣連接於該資料接收單元和該硬體加／解密單元，用於判斷由該資料接收單元接收之加密訊框應由該硬體加／解密單元或該主系統進行解密；及

一第二判斷單元，電氣連接於該硬體加／解密單元和該主系統，用於判斷一應加密訊框應由該硬體加／解密單元加密或已由該主系統加密。

2. 如申請專利範圍第1項之加／解密裝置，其中該主系統係一工作站或一個人電腦。

3. 如申請專利範圍第1項之加／解密裝置，其中該第二加／解密對應表可由一程式予以更新或增加。

4. 一種無線區域網路之加／解密裝置，電氣連接至一主系統，該主系統包含一第二加／解密對應表，該第二加／解密對應表之記錄內容包含該主系統可以加／解密之工作站代碼及鑰匙，該加／解密裝置包含：

一資料接收單元，用於接收訊框；

一資料傳送單元，用於傳送訊框；

一硬體加／解密單元，其係依一個加／解密演算法所製作之電路，該硬體加／解密單元包含一第一加／解密對應表，該第一加／解密對應表之記錄內容包含該硬體加／解密單元可以加／解密之工作站代碼及鑰匙；

一第一判斷單元，電氣連接於該資料接收單元和該硬體加／解密單元，用於判斷由該資料接收單元接收之加密訊框應由該硬體加／解密單元或該主系統進行解密；及

一第二判斷單元，電氣連接於該硬體加／解密單元和該主系統，用於判斷一應加密訊框應由該硬體加／解密單元加密或已由該主系統加密。

5. 如申請專利範圍第4項之加／解密裝置，其中該主系統係一工作站或一個人電腦。

6. 如申請專利範圍第4項之加／解密裝置，其中該第二加／解密對應表可由一程式予以更新或增加。

7. 一種無線區域網路之加／解密裝置，包含：

一資料接收單元，用於接收訊框；

一資料傳送單元，用於傳送訊框；

一硬體加／解密單元，其係依至少一個加／解密演算法所製作之電路，該硬體加／解密單元包含一第一加／解密對應表，該第一加／解密對應表之記錄內容包含該硬體加／解密單元可以加／解密之工作站代碼、加／解密演算法代碼及鑰匙；

一可程式化加／解密單元，包含一第二加／解密對應表，該第二加／解密對應表之記錄內容包含該可程式化加／解密單元可以加／解密之工作站代碼、加／解密演算法代碼及鑰匙；

一第一判斷單元，電氣連接於該資料接收單元和該硬體加／解密單元，用於判斷由該資料接收單元接收之加密訊框應由該硬體加／解密單元或該可程式化加／解密單元進行解密；及

一第二判斷單元，電氣連接於該可程式化加／解密單元和該硬體加／解密單元，用於判斷一應加密訊框應由該硬體加／解密單元加密或已由該可程式化加／解密單元加密。

8. 如申請專利範圍第7項之加／解密裝置，其中該可程式化加／解密單元係由一可程式邏輯元件或一嵌入式系統構成。

9. 如申請專利範圍第7項之加／解密裝置，其中該第二加／解密對應表可由一程式予以更新或增加。

10. 一種無線區域網路之加／解密裝置，包含：

一資料接收單元，用於接收訊框；

一資料傳送單元，用於傳送訊框；

一硬體加／解密單元，其係依一個加／解密演算法所製作之電路，該硬體加／解密單元包含一第一加／解密對應表，該第一加／解密對應表之記錄內容包含該硬體加／解密單元可以加／解密之工作站代碼及鑰匙；

一可程式化加／解密單元，包含一第二加／解密對應表，該第二加／解密對應表之記錄內容包含該可程式化加／解密單元可以加／解密之工作站代碼及鑰匙；

一第一判斷單元，電氣連接於該資料接收單元和該硬體加／解密單元，用於判斷由該資料接收單元接收之加密訊框應由該硬體加／解密單元或該可程式化加／解密單元進行解密；及

一第二判斷單元，電氣連接於該可程式化加／解密單元和該硬體加／解密單元，用於判斷一應加密訊框應由該硬體加／解密單元加密或已由該可程式化加／解密單元加密。

11. 如申請專利範圍第10項之加／解密裝置，其中該可程式化加／解密單元係由一可程式邏輯元件或一嵌入式系統構成。

12. 如申請專利範圍第10項之加／解密裝置，其中該第二加／解密對應表可由一程式予以更新或增加。

13. 一種無線區域網路之解密方法，包含下列步驟：

判斷收到之訊框為密文或原文；

若該訊框為密文，則判斷一硬體解密單元是否可解密；及

若該硬體解密單元可解密該訊框，則由該硬體解密單元進行解密，否則將該訊框傳送至一可程式化解密單元進行解密。

14. 如申請專利範圍第13項之解密方法，其中該可程式化解密單元係由一工作站、一個人電腦、一可程式邏輯元件或一嵌入式系統構成。

15. 如申請專利範圍第13項之解密方法，其中該硬體解密單元包含一第一解密對應表，該可程式化解密單元包含一第二解密對應表，該第一和該第二解密對應表之記錄內容包含其可以解密之工作站代碼及鑰匙。

16. 如申請專利範圍第13項之解密方法，其中該第二解密對應表可由一程式予以更新或增加。

17. 一種無線區域網路之加密方法，包含下列步驟：

判斷要傳送之訊框是否需要加密；

若需加密，判斷一硬體加密單元可否加密；及

若該硬體加密單元可加密該訊框，由該硬體加密單元進行加密，否則由一可程式化加密單元進行加密。

18. 如申請專利範圍第17項之加密方法，其中該硬體加密單元包含一第一加密對應表，該可程式化加密單元包含一第二加密對應表，該第一和該第二加密對應表之記錄內容包含其可以加密之工作站代碼及鑰匙。

19. 如申請專利範圍第17項之加密方法，其中該可程式化加密單元係由一工作站、一個人電腦、一可程式邏輯元件或一嵌入式系統構成。

20. 如申請專利範圍第17項之加密方法，其中該第二加密對應表可由一程式予以更新或增加。

拾壹、圖式

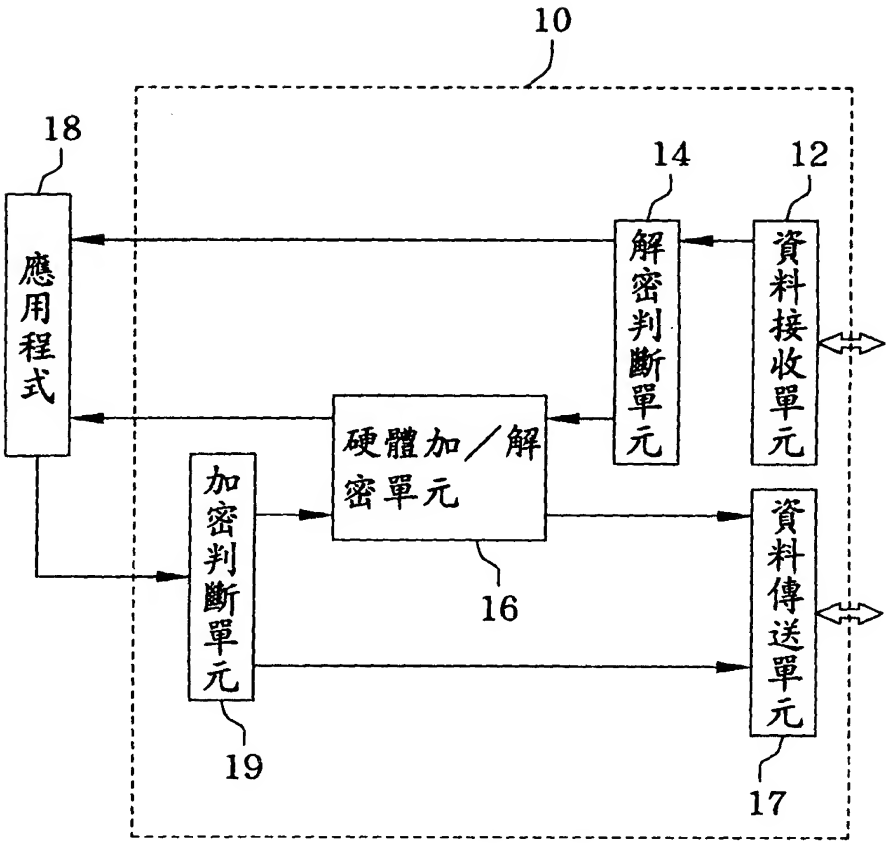

圖 1（習知技藝）

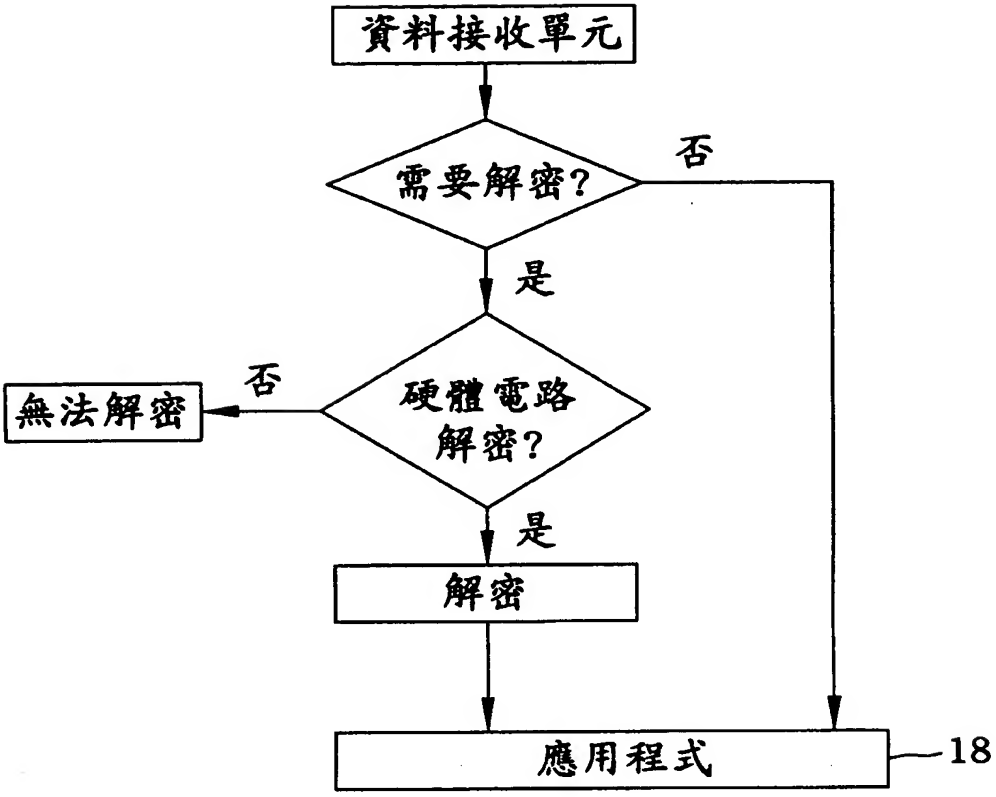

圖 2（習知技藝）

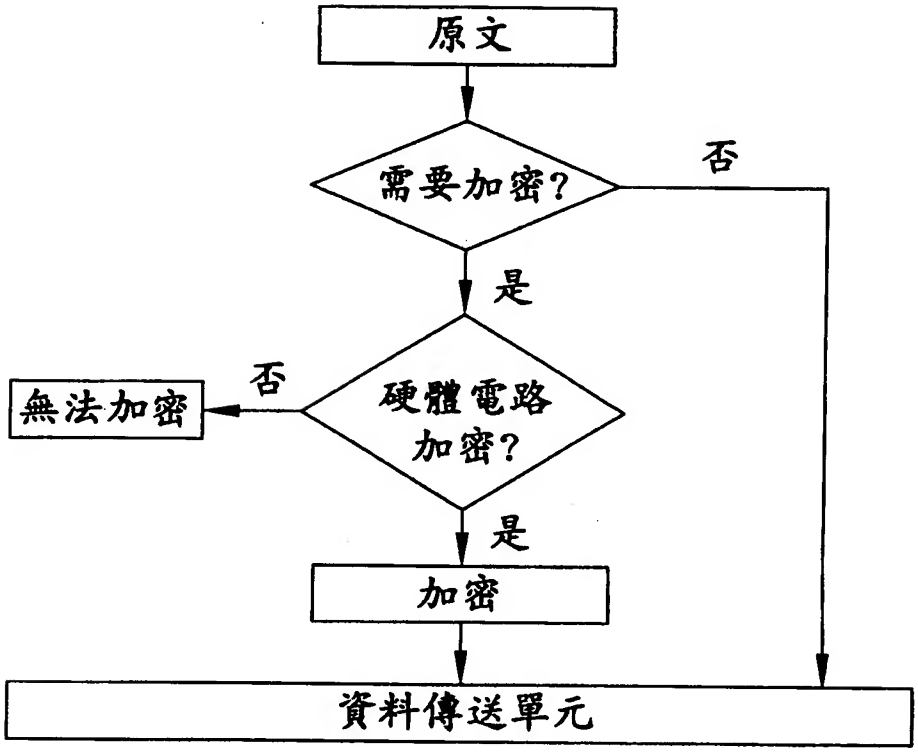

圖 3（習知技藝）

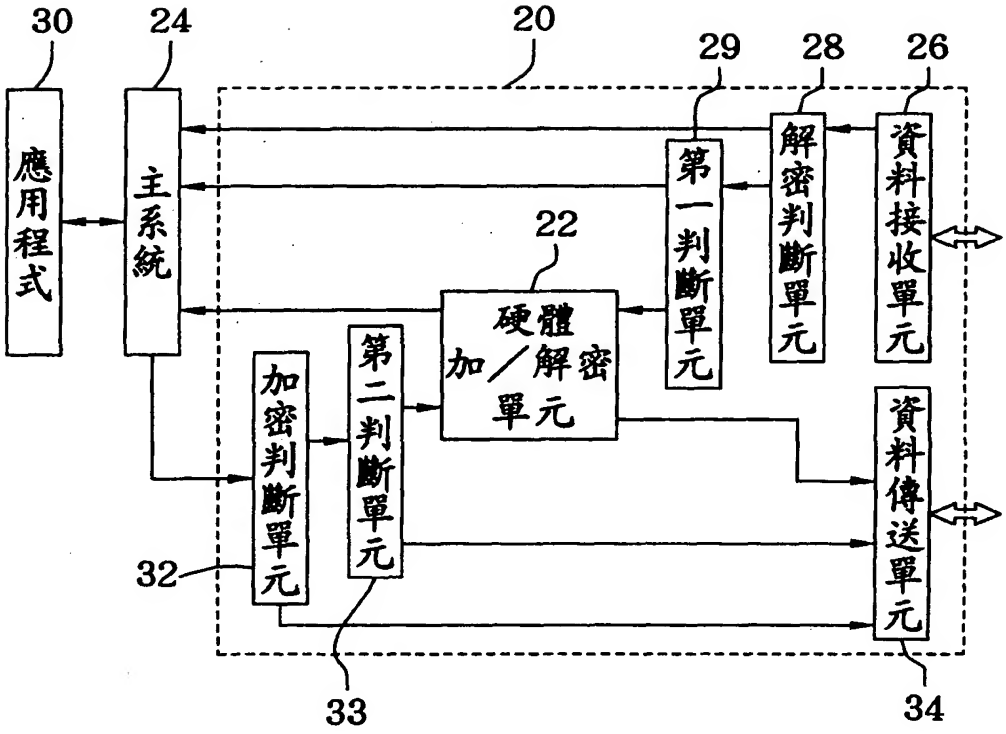
30
24
20
29
28
26
應用程式
主系統
第一判斷單元
解密判斷單元
資料接收單元
22
硬體加/解密單元
第二判斷單元
加密判斷單元
資料傳送單元
32
33
34

圖 4

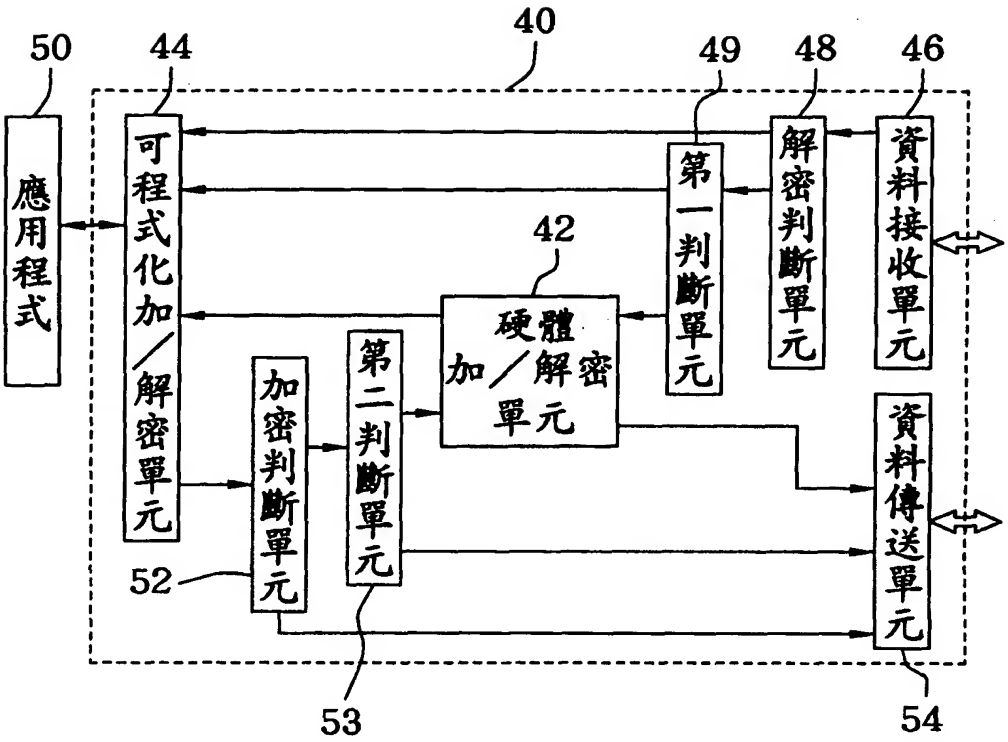
50
44
40
49
48
46
應用程式
可程式化加／解密單元
第一判斷單元
解密判斷單元
資料接收單元
42
硬體加／解密單元
加密判斷單元
第二判斷單元
資料傳送單元
52
53
54

圖 5

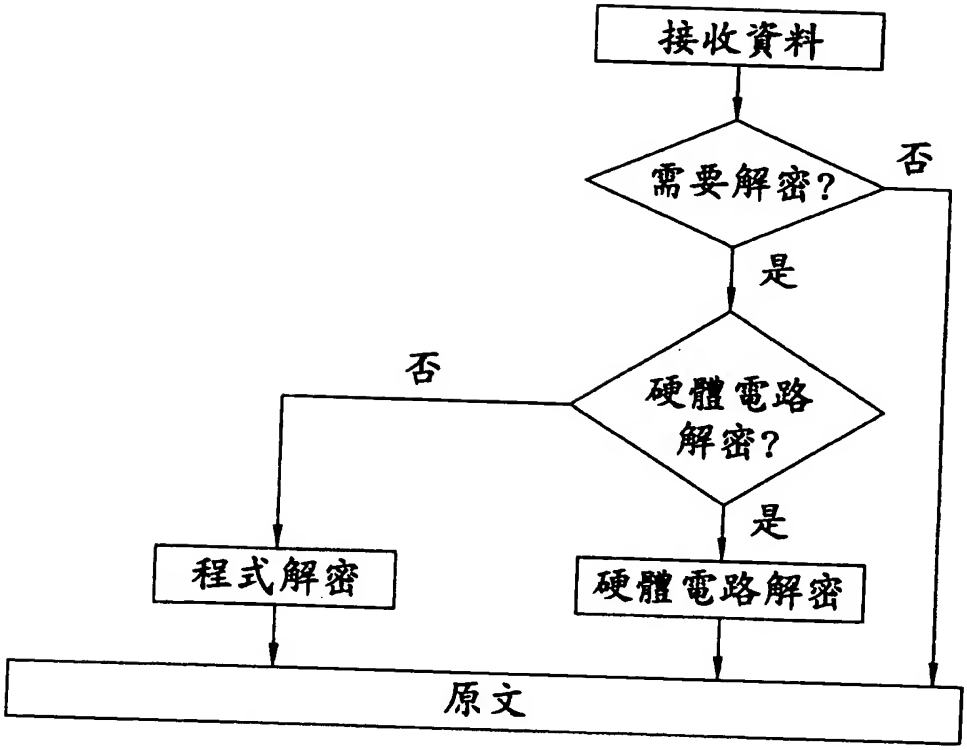

圖 6

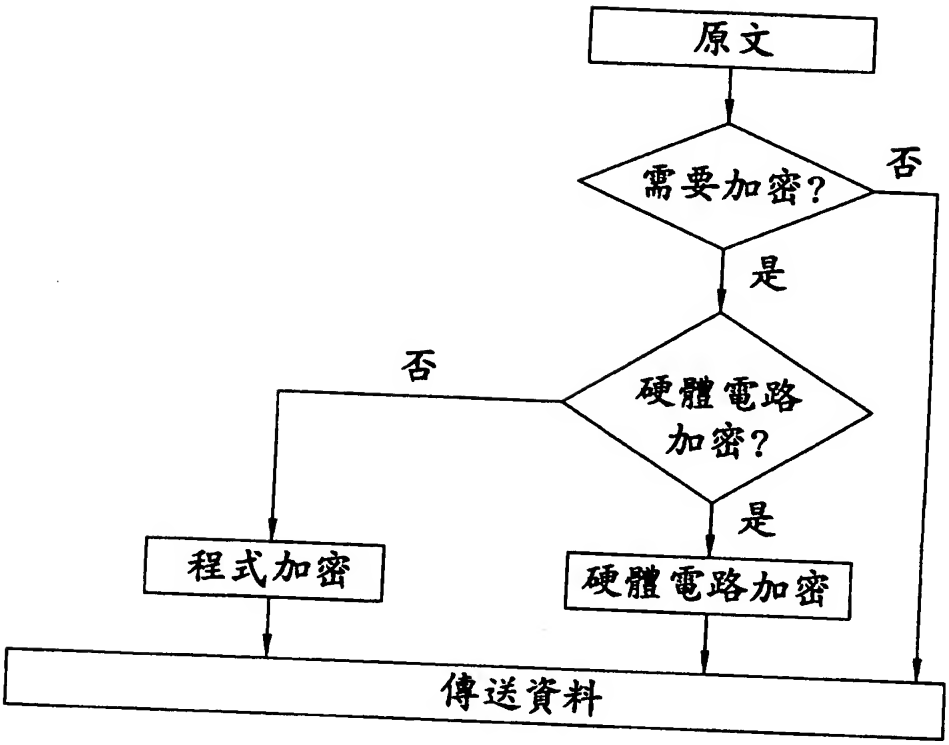

圖 7